WHAT IS CLAIMED IS:1. A domain authentication method for exchanging content between devices, comprising the steps of:

setting domain identification information into a predetermined device connected on one of a wired network and a wireless network, and

generating a domain secret key using the set domain identification information.

2. A domain authentication method for exchanging content between devices, comprising the steps of:

setting domain identification information into a predetermined device connected on one of a wired network and a wireless network, and

generating a domain secret key using the set domain identification information and predetermined device identification information.

3. A domain authentication method for exchanging content between devices, comprising:

a first step of setting domain identification information into a predetermined device connected on one of a wired network and a wireless network;

a second step of generating a domain secret key using the set domain identification information and predetermined device identification information;

a third step of generating a predetermined first code value and transmitting a first packet encrypted with the first code value using the domain secret key generated in the second step;

a fourth step of receiving a second packet that is encrypted with the first code value, which has been decrypted from the first encrypted packet using the domain secret key generated in the second step, and a second code value generated by another device; and

a fifth step of decrypting the second packet received in the fourth step by using the domain secret key generated in the second step and determining whether a specific bit frame of the decrypted second packet is equal to the predetermined first code value generated in the third step.

4. The method as claimed in claim 3, wherein the domain secret key is set as a resultant value of a cryptographic one-way function whose input variables are the domain identification information and the device identification information.

5. The method as claimed in claim 3, wherein the domain secret key is set as a resultant value of a hash function whose input variables are the domain identification information and the device identification information.

6. The method as claimed in claim 3, wherein the first and second code values are predetermined bits of random numbers generated by the devices themselves, respectively.

7. The method as claimed in claim 3, wherein the fifth step further comprises the step of generating a session key to be used for content encryption when the specific bit frame of the second decrypted packet is equal to the predetermined first code value generated in the third step, or terminating a domain authentication process when the specific bit frame is not equal to the first code value.

8. The method as claimed in claim 3, wherein the fifth step further comprises the step of transmitting another specific bit frame, which is based on the second decrypted packet, when the specific bit frame of the decrypted packet is equal to the predetermined first code value generated in the third step.

9. A domain authentication method for exchanging content between devices, comprising;

a first step of performing mutual authentication for the devices using device identification information;

a second step of setting domain identification information into a predetermined device connected on one of a wired network and a wireless network;

a third step of generating a domain secret key using the set domain identification information and the predetermined device identification information;

a fourth step of generating a predetermined first code value and transmitting a first packet encrypted with the first code value using the domain secret key generated in the third step;

a fifth step of receiving a second packet that is encrypted with the first code value, which has been decrypted from the first encrypted packet using the domain secret key generated in the third step, and a second code value generated by another device; and

a sixth step of decrypting the second packet received in the fifth step by using the domain secret key generated in the third step and determining whether a specific bit frame of the decrypted second packet is equal to the predetermined first code value generated in the fourth step.

10. The method as claimed in claim 9, wherein the domain secret key is set as a resultant value of a cryptographic one-way function whose input variables are the domain identification information and the device identification information.

11. The method as claimed in claim 9, wherein the domain secret key is set as a resultant value of a hash function whose input variables are the domain identification information and the device identification information.

12. The method as claimed in claim 9, wherein the first and second code values are predetermined bits of random numbers generated by the devices themselves, respectively.

13. The method as claimed in claim 9, wherein the sixth step further comprises the step of generating a session key to be used for content encryption when the specific bit frame of the second decrypted packet is equal to the predetermined first code value generated in the fourth step, or terminating a domain authentication process when the specific bit frame is not equal to the first code value.

14. The method as claimed in claim 9, wherein the sixth step further comprises the step of transmitting another specific bit frame, which is based on the second decrypted packet, when the specific bit frame of the decrypted packet is equal to the predetermined first code value generated in the fourth step.